IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

Please CANCEL claims 11-19 without prejudice or disclaimer in accordance with the following:

1. (PREVIOUSLY PRESENTED) A data generating apparatus, comprising:

an input device inputting a condition specified by a user for designating a finite field corresponding to a mathematical finite aggregate in which four arithmetical operations are defined, a number of elements of the finite aggregate being expressed as p^m with p and m as a prime number and a positive integer indicating an extension degree, respectively;

a generation device generating a plurality of random numbers based on the inputted condition, generating a plurality of candidates for expression data of the finite field by using the generated random numbers, and checking whether each of the candidates applies to the expression data of the finite field; and

an expression data storage device storing candidates which apply to the expression data of the finite field.

2. (ORIGINAL) The data generating apparatus according to claim 1, further comprising an operation device performing a finite field operation based on the expression data stored in said expression data storage device.

3. (PREVIOUSLY PRESENTED) The data generating apparatus according to claim 1, wherein when a bit length of the prime number is inputted as the condition, said generation device automatically generates prime number data corresponding to the bit length and stores the generated prime number data in said expression data storage device.

4. (PREVIOUSLY PRESENTED) The data generating apparatus according to claim 1, wherein when the extension degree is inputted as the condition, said generation device automatically generates irreducible polynomial data corresponding to the extension degree and stores the irreducible polynomial data in said expression data storage device.

5. (PREVIOUSLY PRESENTED) The data generating apparatus according to claim 4, wherein when an instruction using an optimal normal basis is inputted, said generation device automatically generates irreducible polynomial data for an optimal normal basis corresponding to the extension degree and stores the irreducible polynomial data for an optimal normal basis in said expression data storage device.

6. (ORIGINAL) The data generating apparatus according to claim 1, further comprising a fixed data storage device storing one or more pieces of predetermined expression data of a finite field,

said generation device stores expression data of a finite field corresponding to the condition in said expression data storage device if there is the expression data of a finite field corresponding to the condition in the fixed data storage device, and said generation device automatically generates expression data of a finite field corresponding to the condition if there is no expression data of a finite field corresponding to the condition in the fixed data storage device.

7. (PREVIOUSLY PRESENTED) The data generating apparatus according to claim 1, further comprising:

a designation device designating expression data of a finite field; and

a verifier device verifying whether the designated expression data are suitable, the verifier device storing designated expression data in said expression data storage device if the designated expression data are suitable, and the verifier device asks the designation device for other expression data if the designated expression data are not suitable.

8. (PREVIOUSLY PRESENTED) A computer-readable storage medium on which is recorded a program enabling a computer to execute a process, said process comprising:

specifying a condition designating a finite field corresponding to a mathematical finite aggregate in which four arithmetical operations are defined, a number of elements of the finite aggregate being expressed as p^m with p and m as a prime number and a positive integer indicating an extension degree, respectively;

generating a plurality of random numbers based on the specified condition;

generating a plurality of candidates for expression data of the finite field by using the generated random numbers;

checking whether each of the candidates applies to the expression data of the finite field; and

outputting the candidates which apply to the expression data of the finite field.

9. (PREVIOUSLY PRESENTED) A data generating method, comprising:

designating a condition for designating a finite field corresponding to a mathematical finite aggregate in which four arithmetical operations are defined, a number of elements of the finite aggregate being expressed as p^m with p and m as a prime number and a positive integer indicating an extension degree, respectively;

generating a plurality of random numbers based on the inputted condition;

generating a plurality of candidates for expression data of the finite field by using the generated random numbers;

checking whether each of the candidates applies to the expression data of the finite field; and

supplying the candidates which apply to the expression data of the finite field to a finite field operation apparatus.

10. (PREVIOUSLY PRESENTED) A data generating apparatus, comprising:

inputting means for inputting a condition for designating a finite field corresponding to a mathematical finite aggregate in which four arithmetical operations are defined, a number of elements of the finite aggregate being expressed as p^m with p and m as a prime number and a positive integer indicating an extension degree, respectively;

generating means for generating a plurality of random numbers based on the inputted condition;

generating means for generating a plurality of candidates for expression data of the finite field by using the random numbers;

checking means for checking whether each of the candidates applies to the expression data of the finite field; and

expression data storing means for storing candidates which apply to the expression data of the finite field.

11. -19. (CANCELLED)